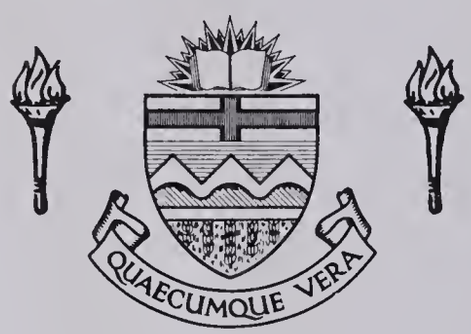


THE UNIVERSITY OF ALBERTA

RELEASE FORM

NAME OF AUTHOR Brett Gordon Giles

TITLE OF THESIS The Unit Groups of Certain Group Rings

DEGREE FOR WHICH THESIS WAS PRESENTED Master of Science

YEAR THIS DEGREE GRANTED 1981

THE UNIVERSITY OF ALBERTA

The Unit Groups of Certain Group Rings

by

Brett Gordon Giles

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES AND RESEARCH

IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE

OF Master of Science

IN

Mathematics

EDMONTON, ALBERTA

FALL, 1981

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research, for acceptance, a thesis entitled The Unit Groups of Certain Group Rings submitted by Brett Gordon Giles in partial fulfilment of the requirements for the degree of Master of Science in Mathematics.

Abstract.

This thesis deals with the problem of describing the unit group of specific group rings over the integers. After a brief introduction to remind one of some of the properties of the group ring, we start to discuss the unit groups. A few of the basic results as presented by Sehgal [6], Chapter 2, are shown. After this introduction, we talk more specifically.

The first method to determine a unit group is then discussed. It is a general method, applicable to any group. However, in practice, we see that it is unsuitable for any but a small number of groups. In this section we talk in an expository manner as the proofs of the results are normally very dependent on the particular group. The ones presented by this method later on are S_3, D_4, D_6 and A_4.

Next, we present the method for groups of order p^3, where p is an odd prime. These come from the paper by Ritter and Sehgal [5]. In this paper, they also present a method for determining the unit group of a particular group of order p^n. This will not be treated here. I consider both non-abelian groups of order p^3 and descriptions of the unit groups of both of their respective group rings are presented. Later on in the paper, I present the method as applied to the groups of order 27.

The last theoretical results are on determining the unit group of the group ring over a group of order pq where $p \equiv 1 (\text{mod } q)$. These results are due to Gallovich, Reiner, and Ullom [7].

The next part deals with presenting actual groups and determining the unit structure of their integral group ring. The first two, S_3 and D_4, are from previous authors. The first was done by Hughes and Pearson [2], the second by C. Polcino-Milies [4]. The case D_6, is new. The last one is merely an expository account of Allen and Hobby's [1] rendering of $\mathcal{U}(\mathbb{Z}A_4)$. Our other concrete examples deal with the two non-abelian groups of order 27 as presented in a paper by Ritter and Sehgal [5].

Table of Contents

I. Preliminaries

A. Generalities

Throughout this paper the term *group ring* shall be taken as follows: The group ring KG of the group G over the ring K (which posesses an identity) is the ring of all formal sums

$$\alpha = \Sigma\lambda(g)g$$

where $g \epsilon G$ and $\lambda(g) \epsilon K$ so that $\text{supp}(\alpha) = \{g \mid \lambda(g) \neq 0\}$ is a finite set.

The ring structure is inherited from the structures of the group and the ring. The operations on KG are defined as follows:

1. $\Sigma\lambda(g)g = \Sigma\mu(g)g \iff$ for all $g \epsilon G$ $\lambda(g) = \mu(g)$
2. $\Sigma\lambda(g)g + \Sigma\mu(g)g = \Sigma(\lambda(g)+\mu(g))g$.
3. $\Sigma\lambda(g)g \cdot \Sigma\mu(g)g = \Sigma\nu(g)g$

where $\nu(g) = \Sigma\lambda(x)\mu(y)$ with the last sum being over all $(x,y) \epsilon G \times G$ with $x \cdot y = g$.

In this paper, we are interested in a particular object that occurs in a group ring. This is the *unit group*. The unit group of a group ring KG is the group of all elements invertible under the multiplication of KG. (It should be noted that the multiplicative identity in KG is the element 1e, where 1 is the multiplicitive identity of K and e the group identity.) Obviously, the unit group of KG contains $\pm G$. More extensive research becomes increasingly difficult.

B. Notation

Throughout this paper the following will be assumed.

$\mathbb{Z}$:- the ring of integers.

$\mathbb{Q}$:- the ring of rational numbers.

R_n :- the ring of n by n matrices with entries from R.

$\langle c \rangle$:- The group generated by the element c.

$\triangle(G,N)$:- $\langle x-1 : x \epsilon N \rangle$ in $\mathbb{Z}G$, where N is normal in G. This also is

$\{ \sum_{g \epsilon G} \mu(g)g \epsilon G : \sum_{x \epsilon N} \mu(gx) = 0 \text{ for all } g \epsilon G \}$.

C. General results.

Proposition.
If G is abelian of order n, then

$$\mathcal{U}\mathbb{Z}G = \pm G \times F,$$

where F is a free abelian group of a determinable rank. This rank is dependent on the number of cyclic subgroups of various orders in G.

The above theorem helps a great deal when dealing with groups, as it is often possible to get a factor or sub-group of your group to fall in this particular category. In particular, this proposition can be used to show that the unit group of $\mathbb{Z}<x>$ where $x^2=1$ is just $\pm<x>$. This fact is used later.

This proposition along with others can be used to prove the more powerful theorem that is stated now.

Theorem.
If G is a torsion group then $\mathcal{U}\mathbb{Z}G = \pm G$ if and only if G is one of

1. an abelian group with $G^4 = \{1\}$ or
2. an abelian group with $G^6 = \{1\}$ or
3. a Hamiltonian 2-group.

This theorem completely characterizes torsion groups that have trivial $\mathcal{U}\mathbb{Z}G$. (A Hamiltonian 2-group is a group of the form E $\times$ quaternions, where $E^2 = 1$).

In conclusion, we note that there are many different areas one can explore when determining unit groups. These range from finding unit groups of particular integral group rings to determining when torsion-free groups have trivial unit groups in their integral group ring.

II. Theoretical considerations

A. Representation theory method.

This method enables us to give a concrete description of the unit groups of certain integral group rings. The first two, S_3 and D_4 were done by Hughes and Pearson, and Polcino-Milies, respectively. The third, which is D_6, was done by myself and involves a minor extension to the method. The last one, A_4, which is included only in an expository way, was done by Allen and Hobby. The general manner in which to apply this method is described below.

Consider the group G. We may use representation theory to determine its non-equivalent irreducible representations. Call these θ_i. These will be maps from $\mathbb{Q}G$ to matrices over $\mathbb{Q}$.

If one takes these θ_i that we have obtained, one may now define a map θ: $\mathbb{Q}G \rightarrow \mathbb{Q}_{i1} \oplus \ldots \oplus \mathbb{Q}_{in}$, by, if $a \in \mathbb{Q}G$, then $\theta(a) = (\theta_1(a),\ldots,\theta_n(a))$. Considering both sides of the mapping as vector spaces over $\mathbb{Q}$, it is readily seen that θ is a linear mapping. Let A be the matrix of θ. It will be noticed that $\theta\mathbb{Z} \subset \oplus\mathbb{Z}_n$. Next, by using the matrix A and its inverse we will be able to deduce a system of linear congruences that give us the restrictions needed for an element of $\bigcirc\mathbb{Z}_n$ to be in $\mathbb{Z}G$. These, together with the fact that a matrix with coefficients in $\mathbb{Z}$ has to have an integral determinant in order to have an integral inverse determine the proper group.

Naturally one sees that a significant problem with this method is the size of the matrix A involved. It is a square matrix of size o(G). Another problem is that we have no guarantee that the system of congruences will lead to a usable situation. Despite these difficulties, the method is sufficiently useful enough to apply it to a few groups of small size.

B. Second Method - Groups of order p^3.

In this section, we intend to study the unit groups of the integral group rings of groups of order p^3, where p is an odd prime. The first type, the commutative groups of order p^3, are known to us.

In dealing with the non-commutative groups of order p^3, we note that there are two non-isomorphic groups of that order. They are:

$H = \langle a,b \mid a^{p^2} = e = b^p,\ b^{-1}ab = a^{p+1} \rangle$ and

$G = \langle a,b,c \mid (a,b) = a^{-1}b^{-1}ab = c,\ ca = ac,\ cb = bc,\ a^p = e = b^p = c^p \rangle$.

Throughout this section we reserve the letters G *and* H *to mean these two groups.*

Fibre product

We must now define the concept of the fibre product.

To understand what a fibre product of rings is, consider the ring R with the two ideals I,J of R such that $I \cap J = 0$. Then we have the diagram

$$\begin{array}{ccc} R & \longrightarrow & R/J \\ \downarrow & & \downarrow \\ R/I & \longrightarrow & R/(I+J) \end{array}$$

Then R is the fibre product of I and J in the sense that

$$R \cong \{(\alpha,\beta) \mid \alpha \in R/I,\ \beta \in R/J, \hat{\alpha} = \tilde{\beta}\},$$

where $\hat{}$ is the map from R/I to R/(I+J) and $\tilde{}$ is the map from R/J to R/(I+J).

From the above we can deduce a fibre product of the unit groups as is given by the following diagram.

$$\begin{array}{ccc} \mathcal{U}(R) & \longrightarrow & \mathcal{U}(R/J) \\ \downarrow & & \downarrow \\ \mathcal{U}(R/I) & \longrightarrow & \mathcal{U}(R/(I+J)) \end{array}$$

Use of Fibre Product

In this section, we are going to apply this to the Group Ring ZX with $J = \triangle(X,N)$ as the kernel of the natural homomorphism of $ZX \to ZX/N$ with N normal in X and $I = \hat{N}ZG$, where $N = \sum_{x \in N} x$. From here on in, we shall write $\hat{x}$ for $\hat{<x>}$.

Pseudo-diagonals of matrices.

To present the proofs of this section, we will need to number certain matrices by their pseudo-diagonals. If the $n \times n$ matrix $A = [a_{ij}]$ is considered, then the j-th pseudo-diagonal is given by the elements

$$a_{1,j+1}, a_{2,j+2}, \ldots, a_{n-1,j-1}, a_{n,j},$$

where the second subscript is considered modulo n and $j = 0,1,2,3,\ldots,n-1$.

Some of the matrices that we will be dealing with from here on will be numbered via their pseudo-diagonals. As an example the matrix $B=[b_{i,j}]$, if numbered by pseudo-diagonals means that the element $b_{i,j}$ is located on the i-th pseudo-diagonal at the j-th spot. When using this indexing scheme, we have $0\leq i,j\leq n-1$.

For convenience, since we will be dealing with many diagonal-like matrices, we introduce the following notation:

$$A = PDIAG_i(x_0,...,x_{n-1})$$

will represent the $n\times n$ matrix that has the elements $x_0,...,x_{n-1}$ on the i-th pseudo-diagonal and zeroes elsewhere. If we are talking of the 0-th pseudo-diagonal, we then mean the main diagonal and refer to it as

$$A = DIAG(x_0,...,x_{n-1}).$$

Preliminary propositions.

Throughout this section we let ω denote a primitive p-th root of unity.

Proposition 1.

Suppose $x_0,...,x_{p-1} \in \mathbb{Z}[\omega]$ then there exists $t_i \in \mathbb{Z}[\omega]$ satisfying

$$\sum_{i=0}^{p-1} t_i\omega^{ji}=x_j,\ 0\leq j\leq p-1$$

if and only if

$$\sum_{i=0}^{p-1} x_i\omega^{ki}\in p\mathbb{Z}[\omega] \text{ for all } 0\leq k\leq p-1$$

Proof.

The system of equations is equivalent to

$$[t_0,...,t_{p-1}]W = [x_0,...,x_{p-1}]$$

where $W=[a_{kl}]$, with $a_{kl} = \omega^{(k-1)(l-1)}$. Now as W is a character matrix, the orthogonality relations of a primitive root of unity tell us that

$$W^{-1} = (1/p)[a_{kl}^{-1}].$$

Our system is equivalent to

$$[t_0,...,t_{p-1}] = [x_0,...,x_{p-1}]W^{-1}.$$

Therefore, there exists a solution if and only if we have

$$(1/p)\sum_{i=0}^{p-1} \omega^{-ik}x_i \in \mathbb{Z}[\omega]$$

for all $0 \leq k \leq p-1$. This, of course, is the same as saying

$$\sum_{i=0}^{p-1} \omega^{ik}x_i \in p\mathbb{Z}[\omega],\ 0 \leq k \leq p-1.$$

Proposition 2.
Let A and B be $p \times p$ matrices over $\mathbb{Q}[\omega]$, with $A = DIAG(1,\omega,\omega^2,...,\omega^{p-1})$ and B as the matrix with ones on pseudo-diagonal number one, (where numbering of pseudo-diagonals start at zero) and zeroes elsewhere, that is $B = PDIAG_1(1,1,...,1)$.

Then the $\mathbb{Z}[\omega]$ span of the matrices $\{A^iB^j, 0 \leq i,j \leq p-1\}$ consists of all elements of the form $M=[x_{ij}]$, where the numbering is via the pseudo-diagonals, and such that for each j,k with $0 \leq j,k \leq p-1$ we have

$$\sum_{i=0}^{p-1} x_{ji}\omega^{ki} \in p\mathbb{Z}[\omega]$$

Proof.
We see that for a fixed j, the matrices A^iB^j, $0 \leq i,j \leq p-1$, have non-zero entries only in the j-th psuedo-diagonal. The vector $(x_0,x_1,...,x_{p-1})$ in $\mathbb{Z}[\omega]$ is a diagonal in the span of $\{A^iB^j\}$ if and only if there exists $t_i \in \mathbb{Z}[\omega]$ such that

$$\sum_{i=0}^{p-1} t_iA^i = DIAG(x_0,x_1,...,x_{p-1})$$

This, we see, means that

$$\sum_{i=0}^{p-1} t_i\omega^{ji} = x_j,\ 0 \leq j \leq p-1$$

and now applying the last proposition we have our answer.

Proposition 3.
Let $o_1 \subset o_2$ be $\mathbb{Z}$-orders in a rational algebra. Then, if an element $\alpha \in o_1$ has an inverse in o_2,

then α already has an inverse in o_1.

Proof.
As groups, we have that the indices behave in the following manner:

$$(o_2:\alpha o_1) = (\alpha o_2:\alpha o_1) \leq (o_2:o_1)$$

which implies that $\alpha o_1 = o_1$, and therefore shows us that α is a unit in o_1.

Now we digress before continuing with our list of propositions. Let us recall our group H with the two generators a and b. Let us write $c = a^{-1}b^{-1}ab = a^{p^2}$. Then we have $H' = <c>$ of order p. Thus $\tilde{H} = H/<c> = <\tilde{a}> \times <\tilde{b}>$. As before, ω is a primitive p-th root of unity. Then

$$\mathbb{Q}H \cong \mathbb{Q}\tilde{H} \oplus \mathbb{Q}(\omega)_p$$

As well as this we have

$$\mathbb{Q}\tilde{H} \cong \mathbb{Q}H/\triangle(H,<c>) \cong \mathbb{Q}H\hat{c} \text{ and}$$
$$\mathbb{Q}(\omega)_p \cong \mathbb{Q}H/\hat{c}\mathbb{Q}H.$$

Clearly this gives us

$$\mathbb{Z}H/\triangle(H,<c>) \cong \mathbb{Z}\tilde{H} \text{ and the mapping}$$
$$\mathbb{Z}H \to \mathbb{Z}\tilde{H} \oplus \mathbb{Z}[\omega]_p.$$

We note that this map is onto the first component. Let us proceed with the calculation of the map with respect to the second component. We easily see that

$$\hat{c}\mathbb{Z}H + (1-c)\mathbb{Z}H = p\mathbb{Z}H + (1-c)\mathbb{Z}H$$

Also, it is obvious that

$$\hat{c}\mathbb{Z}H \cap (1-c)\mathbb{Z}H = 0.$$

Thus, it is obvious that we have the fibre product

$$\begin{array}{ccc} \mathbb{Z}H & \longrightarrow & \mathbb{Z}\tilde{H} \\ \downarrow & & \downarrow \\ \mathbb{Z}H/\hat{c}\mathbb{Z}H & \longrightarrow & \mathbb{Z}\tilde{H}/p\mathbb{Z}\tilde{H} \end{array}$$

with all the maps being natural.

The $p \times p$ matrices $A = PDIAG_1(1,1,\ldots,1,\omega)$ and $B = DIAG(1,\omega,\omega^2,\ldots,\omega^{p-1})$ obviously satisfy the relations $A^p = \omega I$, $B^p = I$, $B^{-1}AB = A^{p^2+1}$.

The matrices $\{B^jA^i \mid 0\leq i,j\leq p-1\}$ are linearly independant over $\mathbb{Z}[\omega]$ as is shown in the following: Assume

$$\sum_{i,j} z_{ij}B^iA^j = 0$$

As A^j has non-zero entries only in the j-th pseudo-diagonal we have

$$\sum_i z_{ij}B^iA^j = 0 \text{ for each } j,\ 0\leq j\leq p-1.$$

As A is a non-singular matrix we have that

$$\sum_i z_{ij}B^i = 0,$$

which immediately implies that $z_{ij} = 0$ for all $0\leq i,j\leq p-1$.

Let $T=\mathbb{Z}H/\hat{c}\mathbb{Z}H$, and Sp be the $\mathbb{Z}[\omega]$-span of the matrices $\{B^iA^j 0\leq i,j\leq p-1\}$, from above. The claim here is that $T \cong Sp$. Consider the map

$$\phi:\mathbb{Z}H\rightarrow Sp,\ \phi(a) = A,\ \phi(b) = B.$$

As $\hat{c} = (1+c+c^2+...+c^{p-1})$ is mapped by ϕ to $(1+\omega+\omega^2+...+\omega^{p-1})I$, which is zero, we have the induced map $\phi_0:T\rightarrow Sp$.

Since $\phi(a^{pk}a^ib^j) = \omega^kA^iB^j$, we have that ϕ_0 is onto Sp. Also we see that ϕ_0 is 1-1, for if we tensor both T and Sp with $\mathbb{Q}$ we see that both of them have $\mathbb{Q}$-dimension of p^3-p^2.

Proposition 4.
A matrix $Z\epsilon\mathbb{Z}[\omega]$ is in Sp if and only if the matrix $X=Z'$ satisfies

$$\sum_{i=0}^{p-1} x_{ji}\omega^{ki} \epsilon\ p\mathbb{Z}[\omega], \text{ for all } 0\leq j,k\leq p-1.$$

where Z' is obtained from Z by dividing all the entries below the main diagonal by ω.

Proof.
We make the observation that $A^i=PDIAG_i(1,1,...,1,\omega,...,\omega)$, where ω is repeated i times. Thus, to compute Sp it is enough to find the span of $\{B^jA^i: 0\leq i,j\leq p-1\}$ separately for each i. Therefore, all we need do is to find all $\mathbb{Z}[\omega]$ vectors of the form $(z_{i0},...,z_{ip-1})$ such that

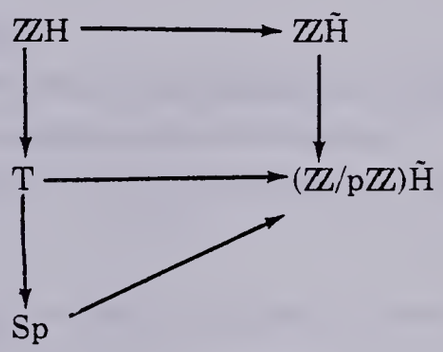
$$\sum_{j=0}^{p-1} t_jB_jDIAG(1,1,...,1,\omega,...,\omega) = DIAG(z_{i0},...,z_{ip-1})$$

which is equivalent to

$$\sum_{j=0}^{p-1} t_j B_j = \mathrm{DIAG}(z_{i0},\ldots,z_{ip-i-1},\omega^{-1}z_{ip-i},\ldots,\omega^{-1}z_{ip-1})$$

And the result therefore follows from proposition 2.

Now let us consider a fibre product of $\mathbb{Z}H$. We have the diagram



with all the maps natural, ϕ_0 being used to map T to Sp. Also,if we let the map from T to $(\mathbb{Z}/p\mathbb{Z})\tilde{H}$ be called θ_1, then let the map ϕ_1:Sp $\rightarrow$ $(\mathbb{Z}/p\mathbb{Z})\tilde{H}$ be defined as $\phi_1=\theta_1\phi_0^{-1}$. Then the diagram above is commutative.

Consider ϕ_1. If $M\epsilon Sp$ we wish to write M as $\Sigma\alpha_{ij}B^iA^j$, $\alpha_{ij}\epsilon\mathbb{Z}[\omega]$, $0\leq i,j\leq p-1$. Let M' be obtained from M by dividing all the elements below the main diagonal by ω. Then the j-th pseudo-diagonal $x_{j,0},\ldots,x_{j,p-1}$ of M' is the same as the main diagonal of $\Sigma\alpha_{ij}B^i$.

We then have

$$[\alpha_{0,j},\ldots,\alpha_{p-1,j}]\ W = [x_{j,0},\ldots,x_{j,p-1}]$$

where $W = [w_{i,j}]$, $w_{i,j} = \omega^{ij}$, $0\leq i,j\leq p-1$.

$$\therefore \alpha_{i,j} = (1/p)\sum_k \omega^{-ij}x_{i,j}.$$

Recalling that we have

$$M = \Sigma\alpha_{i,j}B^iA^j$$

then from the above commutative diagram we have

$$\phi_1(M) = \Sigma\tilde{\alpha}_{i,j}b^ia^j$$

where $\tilde{\alpha}_{i,j}$ is obtained from $\alpha_{i,j}$ by taking $\omega = 1$ and going mod p.

In consideration of Proposition 3, we have the following theorem.

Main result for type 1 groups of order p^3.

Theorem

a) $\mathbb{Z}H \cong \{(\alpha,M) \in \mathbb{Z}\tilde{H} \times \mathbb{Z}[\omega]_p \mid M' \text{ satisfies (*) and } \theta_2(\alpha) = \phi_1(M)\}$.

b) $\mathcal{U}\mathbb{Z}H \cong \{(\alpha,M) \in \mathcal{U}\mathbb{Z}\tilde{H} \times \mathbb{Z}[\omega]_p \mid M \text{ is a unit of } \mathbb{Z}[\omega]_p,\ M' \text{ satisfies (*) and } \theta_2(\alpha) = \phi_1(M)\}$.

In the theorem we have,

(i) M' is obtained from M by dividing every element below the main diagonal by ω, where ω is a primitive p-th root of unity.

(ii) The condition (*) is the one we have encountered many times already

$$\sum_{i=0}^{p-1} x_{j,i}\omega^{ki} \in p\mathbb{Z}[\omega],\ 0 \leq j,k \leq p-1,\ \omega^p = 1.$$

where $\{x_{i,j}\}$ are numbered according to the pseudo-diagonals of M'.

(iii) θ_2: $\mathbb{Z}\tilde{H} \to (\mathbb{Z}/p\mathbb{Z})\tilde{H}$ is the natural map Mod p.

(iv) $\phi_1(M) = \sum_{i,j} \tilde{\alpha}_{i,j}\tilde{b}^i\tilde{a}^j$ where $\alpha_{i,j} = (1/p)\sum_k \omega^{-ik}x_{jk} \in \mathbb{Z}[\omega]$ and $\tilde{\alpha}_{i,j}$ is obtained from $\alpha_{i,j}$ by putting $\omega = 1$ and going mod p.

Groups of type 2 of order p^3.

We now consider our second group of order p^3 which we refer to as G. Recall,

$$G = \langle a,b,c \mid (a,b) = a^{-1}b^{-1}ab = c,\ ca = ac,\ cb = bc,\ a^p = e = b^p = c^p \rangle.$$

We note that the factor commutator group, $\tilde{G} = G/\langle c \rangle$ is elementary abelian of order p^2, $\tilde{G} = \langle \tilde{a} \rangle \times \langle \tilde{b} \rangle$. This gives us the decomposition

$$\mathbb{Q} \cong \mathbb{Q}\tilde{G} \oplus \mathbb{Q}(\omega)_p.$$

In fact, we have

$$\mathbb{Q}\tilde{G} \cong \mathbb{Q}G/\triangle(G,\langle c \rangle) \cong \mathbb{Q}G\hat{c} \text{ and}$$
$$\mathbb{Q}(\omega)_p \cong \mathbb{Q}G/\hat{c}\mathbb{Q}G.$$

Clearly this gives us

$$\mathbb{Z}G/\triangle(G,\langle c \rangle) \cong \mathbb{Z}\tilde{G} \text{ and the mapping}$$
$$\mathbb{Z}G \to \mathbb{Z}\tilde{G} \oplus \mathbb{Z}[\omega]_p$$

with the mapping being onto on the first component. Our next step will be, as before, to compute the projection into the second component. We consider the fibre product diagram

$$\begin{array}{ccc} \mathbb{Z}G & \longrightarrow & \mathbb{Z}\tilde{G} \\ \downarrow & & \downarrow \\ \mathbb{Z}G/\hat{c}\mathbb{Z}G & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})\tilde{G} \end{array}$$

where all the maps are the natural projections excepting the map on the bottom which is

$$\theta_1 : \mathbb{Z}G/\hat{c}\mathbb{Z}G \rightarrow (\mathbb{Z}/p\mathbb{Z})\tilde{G} \text{ with}$$
$$\theta_1(\Sigma z c^i a^j b^k) = \Sigma z \tilde{a}^j \tilde{b}^k, \text{ with } z \in \mathbb{Z}.$$

Twisting of Group Rings

In order to continue, we need to introduce the notion of *twisted* group rings at this point. A twisted group ring is constructed in the same manner as an ordinary group ring except that the definition of multiplication differs. In the twisted group ring, there is a twisting factor that is used to multiply elements.

Let us take the twisted group ring of a ring R and a group G. This is then written as $R^{\circ}G$. Using this notation, it is easy to see that $\mathbb{Z}G/\hat{c}\mathbb{Z}G$ is isomorphic as a ring to the twisted group ring $\mathbb{Z}[\omega]^{\circ}\tilde{G}$ with $\tilde{b}\tilde{a} = \omega\tilde{a}\tilde{b}$. After this identification, we see that the map θ_1 may be written as

$$\theta_1(\Sigma\alpha\tilde{a}^i\tilde{b}^j) = \Sigma\tilde{\alpha}\tilde{a}^i\tilde{b}^j, \ \alpha \in \mathbb{Z}[\omega].$$

where we get $\tilde{\alpha}$ from α by substituting $\omega = 1$, and going mod p.

Let us now define the map ϕ_0 from $\mathbb{Z}[\omega]^{\circ}\tilde{G}$ to $\mathbb{Z}[\omega]_p$ by

$$\tilde{a} \rightarrow A = \mathrm{DIAG}(1,\omega,\ldots,\omega^{p-1}), \quad \tilde{b} \rightarrow B = \mathrm{PDIAG}_1(1,\ldots,1).$$

We note that $BA = \omega AB$ and that $A^p = I = B^p$.

We claim that $\{A^iB^j\}$ is a linearly independent set over $\mathbb{Z}[\omega]$ for $0 \le i,j \le p-1$. This can easily be seen as follows. Let $\alpha_{i,j}$ be in $\mathbb{Z}[\omega]$ for $0 \le i,j \le p-1$. Then we see that

$$\Sigma_i \Sigma_j \alpha_{i,j} A^iB^j = 0 \text{ implies} \Sigma_j \alpha_{i,j} A^iB^j = 0,$$

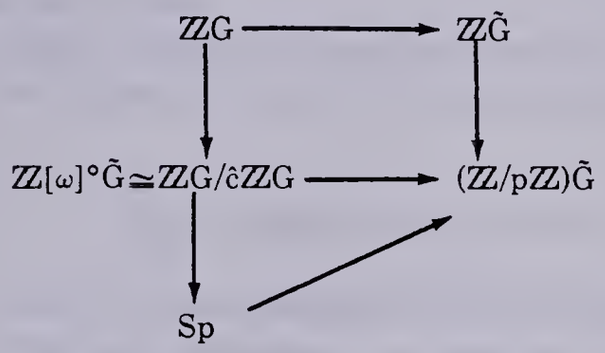
as B^j has non-zero entries only in the j-th diagonal. Since B is non-singular, we may remove the B^j from the above result, which implies that $\alpha_{i,j} = 0$ for all $0 \le i,j \le p-1$. Therefore, we now have that if $Sp = \mathrm{span}\{A^iB^j, 0 \le i,j \le p-1\}$, then

$$\mathbb{Z}G/\hat{c}\mathbb{Z}G \cong \mathbb{Z}[\omega]^{\circ}\tilde{G} \cong Sp.$$

From proposition 2 it follows that

$$Sp = \{M \in \mathbb{Z}[\omega]_p \mid M \text{ satisfies} \sum_{i=0}^{p-1} x_{j,i}\omega^{ki} \in p\mathbb{Z}[\omega] \text{ for all } 0 \leq j,k \leq p-1\}.$$

Let us consider the following fibre product diagram and extension to Sp.



In the above, the map from Sp to $(\mathbb{Z}/p\mathbb{Z})\tilde{G}$ is denoted by ϕ_1 and the map from $\mathbb{Z}G/\hat{c}\mathbb{Z}G$ to Sp is denoted by ϕ_0. Obviously, as before in a similar diagram, we define ϕ_1 to be the map $\theta_1\phi_0^{-1}$.

As before, given M in Sp we wish to find $\phi_0^{-1}(M) \in \mathbb{Z}[\omega]^{\circ}\tilde{G}$. Let $M = \{x_{j,i}\}$ be numbered by the pseudo-diagonals. We wish to find $a_{i,j} \in \mathbb{Z}[\omega]$ such that $\sum_{i,j} a_{i,j}A^iB^j = M$. It is necessary to find $a_{i,j}$ such that

$$\sum_i a_{i,j}A^i = DIAG(x_{j,0},\ldots,x_{j,p-1}),\ 0 \leq j \leq p-1.$$

Again as before we get this is equivalent to the matrix equation

$$[a_{0,j},\ldots,a_{p-1,j}]W = [x_{j,0},\ldots,x_{j,p-1}]$$

where $W = [w_{i,j}]$ numbered by columns and rows starting at zero and $w_{i,j} = \omega^{ij}$. Again, by following the previous procedure, we see that

$$a_{i,j} = (1/p)\sum_{k=0}^{p-1} \omega^{-ki}x_{j,k}.$$

From the above we have that

$$\phi_0^{-1}(M) = \sum_{i,j} a_{i,j}\tilde{a}^i\tilde{b}^j \text{ and } \phi_1(M) = \sum_{i,j} \tilde{a}_{i,j}\tilde{a}^i\tilde{b}^j,$$

where $\tilde{a}_{i,j}$ is obtained from $a_{i,j}$ by substituting $\omega = 1$ and going mod p.

The above constitutes the first part of the next theorem. The second part follows directly from proposition 3 as Sp is an order in $\mathbb{Z}[\omega]_p$.

Main result for type 2 groups of order p^3

Theorem

a) $\mathbb{Z}G \cong \{(\alpha,M) \in \mathbb{Z}\tilde{G} \times \mathbb{Z}[\omega]_p \mid M' \text{ satisfies (*) and } \theta_2(\alpha) = \phi_1(M)\}$.

b) $\mathcal{U}\mathbb{Z}G \cong \{(\alpha,M) \in \mathcal{U}\mathbb{Z}\tilde{G} \times \mathbb{Z}[\omega]_p \mid M \text{ is a unit of } \mathbb{Z}[\omega]_p, M \text{ satisfies (*) and } \theta_2(\alpha) = \phi_1(M)\}$.

In the theorem we have,

(i) θ_2: $\mathbb{Z}\tilde{G} \to (\mathbb{Z}/p\mathbb{Z})\tilde{G}$ is the natural map mod p;

(ii) The condition (*) is the one we have encountered many times already

$$\sum_{i=0}^{p-1} x_{j,i}\omega^{ki} \in p\mathbb{Z}[\omega],\ 0 \leq j,k \leq p-1,\ \omega^p = 1.$$

where $\{x_{i,j}\}$ are numbered according to the pseudo-diagonals of M.

(iii) $\phi_1(M) = \sum \tilde{a}_{i,j}\tilde{a}^i\tilde{b}^j$ where $a_{i,j} = (1/p)\sum_k \omega^{-ki}x_{jk} \in \mathbb{Z}[\omega]$ and $\tilde{a}_{i,j}$ is obtained from $a_{i,j}$ by putting $\omega^{i,j} = 1$ and going mod p.

Concluding remarks on groups of order p^3

This concludes our section on groups of order p^3. It should be noted that there are striking similarities in the derivations for both types of groups. However, the proofs do need to be presented separately due to the underlying differences. In a paper by Sehgal and Ritter[5], the method presented here for type 1 groups of order p^3 is extended to similar type groups of order p^n.

At the end of this paper, I will present examples of the methods shown in this section, using groups of order 27.

C. Third method - Groups of order pq

Generalities

In this section, we shall study the unit group of groups of order pq, where p and q are primes $p \equiv 1 \pmod q$. We shall restrict our attention to the non-abelian group of this order. Recall,

$$G = \langle a,b \mid a^p = b^q = 1, bab^{-1} = a^j,\ j \not\equiv 1 \pmod p,\ j^q \equiv 1 \pmod p \rangle.$$

In this case, we will need to consider the map

$$\sigma: \mathcal{U}\mathbb{Z}G \to \mathcal{U}\mathbb{Z}\langle b \rangle \cong \mathbb{Z}(G/\langle a \rangle).$$
$$\sigma(a) = 1,\ \sigma(b) = b.$$

Let us denote by $\mathcal{N}$ the units of the kernel of this map. We note that any unit of $\mathbb{Z}G$ can be written as the product of an element of $\mathcal{N}$ and a unit of $\mathbb{Z}\langle b \rangle$.

Now since the units of $\mathbb{Z}<b>$ may be assumed to be known to us and we have the equation

$$ba = a^j b$$

we only need to determine the set $\mathcal{N}$.

Let ω be a primitive p-th root of unity. Then the field $k = \mathbb{Q}(\omega)$ is a cyclic extension of $\mathbb{Q}$ of order p-1. Let k_0 be the fixed field of the automorphism $t:\omega \longrightarrow \omega^j$. Then k_0 is of degree (p-1)/q over $\mathbb{Q}$. For any element α of k let

$$\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(q-1)}$$

be the succesive applications of the automorphism t.

Let R and R_0 denote the rings of integers of k and k_0, respectively. We note that R is a free R_0-module with the basis

$$1, \chi, \chi^2, \ldots, \chi^{q-1}$$

where

$$\chi = \omega - 1.$$

is the prime in R over the rational prime p. The corresponding prime in R_0 is

$$\chi_0 = (\omega-1)\ (\omega^2-1)\ \ldots\ (\omega^{q-1}-1)$$

As $(\omega^i-1)/(\omega-1)$ is a unit, we have that $(\chi_0) = (\chi^q)$ as ideals.

Recall from number theory that in the above situation we have that

$$\mathbb{Z}/p\mathbb{Z} \cong R_0/\chi_0 R_0 \cong R/\chi R.$$

Therefore, in particular, we have that each element of R modulo χ is congruent to a rational integer.

At this point, we present a lemma.

Lemma.

Suppose $\alpha \epsilon R$, with $\alpha \equiv s \pmod{\chi}$, with $s \epsilon \mathbb{Z}$. Then α can be written uniquely as

$$\alpha = a_0 + a_1\omega + \ldots + a_{p-1}\omega^{p-1}.$$

with $\sum a_i = s$, and the $a_i \epsilon \mathbb{Z}$.

Proof.

Write

$$\alpha = c_0 + c_1\omega + c_2\omega^2 + \ldots + c_{p-1}\omega^{p-1}$$

where the c_i are rational integers. Since $\alpha \equiv s \pmod{\chi}$. we therefore have

$$(\dagger) \qquad c_0 + c_1 + \ldots + c_{p-1} \equiv s \pmod{p}$$

In full generality the first equation may be rewritten as

$$\alpha = (c_0+m)+(c_1+m)\omega+(c_2+m)\omega^2+\ldots+(c_{p-1}+m)\omega^{p-1}$$

where m is a rational integer. The sum of the new coefficients is s if and only if

$$c_0+c_1+\ldots+c_{p-1}+pm = s.$$

Considering (†) above, the relation gives us a unique value for m such that the equality does hold.

The unit group as matrices over R.

Recall that it is obvious that $\mathbb{Z}G \cong \mathbb{Z}\langle a\rangle\langle b\rangle$ and, therefore, an element x of $\mathbb{Z}G$ can be written as

$$x(a,b) = x_0(a)+x_1(a)b+\ldots+x_{q-1}(a)b^{q-1}$$

where $x_i(a)$ is an element of $\mathbb{Z}\langle a\rangle$. Therefore, if x,y,z are in $\mathbb{Z}G$, written as above, and $z = x \bullet y$, then we would have (upon recalling the definition of multiplication in a group ring) the equations

$$\begin{aligned}
z_0(a) &= x_0(a)y_0(a)+x_1(a)y_{q-1}(a^j)+\ldots+x_{q-1}(a)y_1(a^{jq-1})\\
z_1(a) &= x_0(a)y_1(a)+x_1(a)y_0(a^j)+\ldots+x_{q-1}(a)y_2(a^{jq-1})\\
&\bullet\\
&\bullet\\
&\bullet\\
z_{q-1}(a) &= x_0(a)y_{q-1}(a)+x_1(a)y_{q-2}(a^j)+\ldots+x_{q-1}(a)y_0(a^{jq-1})
\end{aligned}$$

Recalling that $\mathbb{Z}\langle a\rangle \cong \mathbb{Z}[X]/(X^p-1)$ we can therefore associate to an element x(a,b) of $\mathbb{Z}G$ the elements

$$\alpha_0 = x_0(\omega),\ \alpha_1 = x_1(\omega),\ldots,\ \alpha_{q-1} = x_{q-1}(\omega),$$

with α_i in R.

Consider the matrix

$$A = \begin{bmatrix}
\alpha_0, \alpha_1, \ldots, \alpha_{q-1}\\
\alpha_{q-1}^{(1)}, \alpha_0^{(1)}, \ldots, \alpha_{q-2}^{(1)}\\
\bullet \qquad \bullet\\
\bullet \qquad \bullet\\
\bullet \qquad \bullet\\
\alpha_1^{(q-1)}, \alpha_2^{(q-1)}, \ldots, \alpha_0^{(q-1)}
\end{bmatrix}$$

with entries in R. We shall call matrices with this form matrices of type 1.

From our previous calculations, we see that the obvious map $x(a,b) \to A$ is a homomorphism from $\mathbb{Z}G$ into the matrices of type 1.

Let us consider what happens when A is invertible in R. Denoting the first row of A^{-1} by $\beta_0,\ldots,\beta_{q-1}$ and we would then have the system of equations

$$\beta_0\alpha_0 + \beta_1\alpha_{q-1}^{(1)}+\ldots+\beta_{q-1}\alpha_1^{(q-1)}=1$$
$$\beta_0\alpha_1 + \beta_1\alpha_0^{(1)} + \beta_{q-1}\alpha_2^{(q-1)}=0$$
$$\vdots$$
$$\beta_0\alpha_{q-1} + \beta_1\alpha_{q-2}^{(1)} + \beta_{q-1}\alpha_0^{(q-1)}=0$$

If we apply the automorphism $t:\omega\rightarrow\omega^j$ to these relations successively we see that

$$A^{-1}=\begin{bmatrix} \beta_0, \beta_1, \ldots, \beta_{q-1} \\ \beta_{q-1}^{(1)}, \beta_0^{(1)}, \ldots, \beta_{q-2}^{(1)} \\ \vdots \quad\quad \vdots \\ \beta_1^{(q-1)}, \beta_2^{(q-1)},\ldots,\beta_0^{(q-1)} \end{bmatrix}$$

is once again of the same type. Therefore, our conclusion is that the invertible matrices of the type 1 form a group.

Let us restrict the homomorphism from ZG to type 1 matrices down to $\mathcal{N}$. Let us further restrict it to matrices of type 1 that satisfy the following conditions:

(i) $\alpha_0\equiv 1, \alpha_1\equiv 0,\ldots,\alpha_{q-1}\equiv 0 \pmod{\chi}$ or $A\equiv I \pmod{\chi}$.
(ii) det A is a unit in R_0.

We claim that the homomorphism is actually an isomorphism. First, we show that it is one-to-one. Let x(a,b) be in $\mathcal{N}$, with x(a,b) being mapped to the identity. Then

$$x_0(\omega)=1,\ x_1(\omega)=0,\ldots,x_{q-1}(\omega)=0.$$

Since x(a,b) is a normalized unit we also have

$$x_0(1)=1,\ x_1(1)=0,\ldots,x_{q-1}(1)=0$$

which means that

$$x_0(a)=1,\ x_1(a)=0,\ldots,x_{q-1}(a)=0.$$

That shows that the map is one-to-one.

We now show that it is onto. Let A be invertible of type 1 and satisfy conditions (i) and (ii). Let B be the inverse of A. Let

$$\alpha_0 = x_0(\omega),\ \alpha_1 = x_1(\omega),\ldots,\alpha_{q-1} = x_{q-1}(\omega).$$

where the $x_i(X)$ are polynomials with rational integer coefficients of degree $\leq$ p-1, the sum of the coefficients of x_i =1, or =0, corresponding to i=0, or i=1,2,...,q-1. Form the element

$$x(a,b) = x_0(a) + x_1(a)b + \ldots + x_{q-1}(a)b^{q-1}$$

and the corresponding element for B

$$y(a,b) = y_0(a) + y_1(a)b + \ldots + y_{q-1}(a)b^{q-1}$$

which is derived in a similiar manner.

Since AB = I we have

$$\sum_{l+m\equiv i(\mathrm{mod}\ p)} x_l(\omega)y_m(\omega) = 1 \text{ or } 0$$

according as to i=0 or i=1,2,3,...,q-1.
Also we see that

$$\sum_{l+m\equiv i(\mathrm{mod}\ p)} x_l(1)y_m(1) = 1 \text{ or } 0$$

according as to i=0 or i=1,2,3,...,q-1. Therefore, x(a,b)y(a,b) = 1. In the same manner as above we see that y(a,b)x(a,b) = 1.

Therefore, we have proven that the subgroup $\mathcal{N}$ of $\mathbb{Z}G$ is isomorphic to the type 1 matrices in R that satisfy conditions (i) and (ii).

The unit group as matrices over R_0

In this section, we continue from where we left off at the end of the last section and extend our description of $\mathcal{N}$.

Let us put

$$\begin{aligned}\delta(X) &= (X-\chi^{(1)})(X-\chi^{(2)})\ldots(X-\chi^{(q-1)}) \\ &= X^{q-1}+\delta_1 X^{q-2}+\ldots+\delta_{q-1}.\end{aligned}$$

Also let

$$\delta = \delta(\chi).$$

Since we obviously have $X-\chi \equiv X \pmod{\chi}$, we have that

$$N_{k/k_0}(X-\chi) \equiv X^q \pmod{\chi_0},$$

and, therefore, if we compare coefficients in $(X-\chi)\delta(X) = N_{k/k_0}(X-\chi)$, we will have

$$(\ddagger) \qquad \delta_i \equiv \chi^i \pmod{\chi_0}.$$

Let $\delta_0 = 1$ and

$$P = \begin{bmatrix} 1 & \chi & \dots & \chi^{q-1} \\ 1 & \chi^{(1)} & \dots & (\chi^{(1)})^{q-1} \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ 1 & \chi^{(q-1)} & \dots & (\chi^{(q-1)})^{q-1} \end{bmatrix}$$

With some work, we can see that P^{-1} is $[p_{i,j}]$ $1 \leq i,j \leq q$, where the numbering is by rows and columns and $p_{i,j} = (\delta_{q-i}/\delta)^{(i-1)}$ where $a^{(0)}$ is, of course, just a.

Let $E = PDIAG_1(1,1,\dots,1)$ be a $q \times q$ matrix. It is quite obvious that $E^{-1} = PDIAG_{q-1}(1,1,\dots,1) = E^{q-1}$. For a matrix M with entries in k, we shall denote by M' the matrix obtained from M by applying the automorphism t to the entries of M. In consideration of this, it is obvious that $P' = EP$, and $(P^{-1})' = P^{-1}E^{-1}$. Therefore if A has its entries in k, then $P^{-1}AP$ has entries in k_0 if and only if

$$A' = E\,A\,E^{-1}.$$

This is equivalent to the matrix A being a type 1 matrix from the previous section. That is

$$A = \begin{bmatrix} \alpha_0, \alpha_1, \dots, \alpha_{q-1} \\ \alpha_{q-1}^{(1)}, \alpha_0^{(1)} \dots, \alpha_{q-2}^{(1)} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ \alpha_1^{(q-1)}, \alpha_2^{(q-1)}, \dots, \alpha_0^{(q-1)} \end{bmatrix}$$

where the elements are in k.

It then follows that the map from A to $X = P^{-1}\,A\,P$ is an isomorphism of the ring of matrices A of type 1 having entries in k with the ring of $q \times q$ matrices X with entries in k_0.

Let $X = [x_{i,j}]$ $0 \leq i,j \leq q-1$. Suppose that X with entries in R_0 satisfies the congruence

$$(\dagger\dagger) \qquad X \equiv \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} \pmod{\chi_0 (= \chi^q)}.$$

Then the entries in the first row of the corresponding matrix $A = P X P^{-1}$ are

$$\alpha_0 = (1/\delta)[\, x_0(\chi)(\delta_{q-1}) + x_1(\chi)(\delta_{q-2}) + \ldots + x_{q-1}(\chi)(\delta_0)] = \beta_0/\delta$$
$$\alpha_1 = (1/\delta^{(1)})[\, x_0(\chi)(\delta_{q-1})^{(1)} + x_1(\chi)(\delta_{q-2})^{(1)} + \ldots + x_{q-1}(\chi)(\delta_0)^{(1)} \,] = \beta_1/\delta^{(1)}$$
$$\vdots$$
$$\alpha_{q-1} = (1/\delta^{(q-1)})[\, x_0(\chi)(\delta_{q-1})^{(q-1)} + x_1(\chi)(\delta_{q-2})^{(q-1)} + \ldots + x_{q-1}(\chi)(\delta_0)^{(q-1)} \,] = \beta_{q-1}/\delta^{(q-1)}.$$

where, for $0 \leq i \leq q-1$,

$$x_i(\chi) = x_{0,i} + x_{1,i}\chi + \ldots + x_{q-1,i}\chi^{q-1} \equiv \chi^i \pmod{\chi^{i+1}},$$

This implies, if we consider the congruences ‡ involving the δ_i's and the congruences that one can derive by successive applications of the automorphism t to them we have

$$\beta_0 \equiv q\chi^{q-1} \pmod{\chi_0}$$

and

$$\beta_i \equiv (\chi^{(i)})^{q-1} + \chi(\chi^{(i)})^{q-2} + \ldots + \chi^{q-2}(\chi^{(i)}) + \chi^{q-1} \pmod{\chi_0}$$

Since δ and its conjugates via the isomorphism t are all associates of χ^{q-1}, this means that the α_i are all elements of R. As well, (mod χ) we will have the following holds true:

$$\delta/\chi^{q-1} = [1-(\chi^{(1)}/\chi)][1-(\chi^{(2)}/\chi)]\ldots[1-(\chi^{(q-1)}/\chi)]$$
$$\equiv (j-1)(j^2-1)\ldots(j^{q-1}-1) \equiv q \pmod{\chi}.$$

Therefore, we have that

$$\alpha_0 = (\beta_0/\delta) \equiv 1 \pmod{\chi}.$$

Since

$$(\chi^{(1)}/\chi)^q - 1 = [(\omega^j-1)/(\omega-1)]^q - 1 \equiv j^q - 1 \equiv 0 \pmod{\chi},$$

therefore, $(\chi^{(1)})^q - \chi^q \equiv 0 \pmod{\chi^{q+1}}$, and therefore, noticing that $\chi^{(1)} - \chi$ is an associate of χ, we have

$$\beta_1 \equiv \left(((\chi^{(1)})^q - \chi^q)/(\chi^{(1)} - \chi)\right) \equiv 0 \pmod{\chi^q},$$

giving us the relation

$$\alpha_1 = \beta_1/\delta^{(1)} \equiv 0 \pmod{\chi}.$$

Similarly, we can continue to show that $\alpha_i \equiv 0 \pmod{\chi}$ for $2 \leq i \leq q-1$.

Now let us do the converse. Suppose we have a matrix A of type 1 with entries in R that satisfy the conditions

$$\alpha_i \equiv 1 \text{ or } 0 \pmod{\chi}$$

depending as $i=0$ or $i=1,2,\ldots,q-1$. Let $X = P^{-1} A P$. Number the matrix X as above, $X=[x_{i,j}]$ $0 \leq i,j \leq q-1$, the numbering according to columns and rows. In consideration of the above, we note that

$$\begin{aligned} x_{i,j} &= \sum_{u,v} (\delta_{q-i-1}/\delta)^{(u)} (\alpha_{q-u+v})^{(u)} (\chi^j)^{(v)} \\ &= \sum_u \left(\sum_v [(\delta_{q-i-1}/\delta)\alpha_{q-u+v} (\chi^j)^{(v-u)}] \right)^{(u)} \\ &= \sum_u \left(\sum_v [(\delta_{q-i-1}/\delta)\alpha_v (\chi^j)^{(v)}] \right)^{(u)} \\ &= \mathrm{Tr}\left((\delta_{q-i-1}/\delta) \sum_v \alpha_v (\chi^j)^{(v)} \right), \end{aligned}$$

where Tr is the trace of k over k_0. Since δ is the different of the extension k over k_0, we have that $x_{i,j}$ is in R_0. As well, in view of the congruences involving the δ_1 and the α_1, we would have that if $j \geq i$,

$$x_{i,j} = \mathrm{Tr}\left((\chi^{q-i-1}/\delta) \sum_v \alpha_v (\chi^j)^{(v)} \right) = \mathrm{Tr}\left((\chi_{q-i-1}/\delta)\alpha_0 \chi^j \right) = \mathrm{Tr}\left(\chi_{q-1+j-i}/\delta \right) \equiv 1 \text{ or } 0 \pmod{\chi_0}$$

according to whether $i=j$ or $i<j$. This means that the matrix X has entries in R_0 satisfying the conditions (‡). Therefore, we have proven the following theorem.

THEOREM.
The subgroup $\mathcal{N}$ of ZG is isomorphic to the group of $q \times q$ matrices X in R_0 that are invertible in R_0 and satisfying the congruences

$$X \equiv \begin{matrix} 1 & & 0 \\ & & \\ * & & 1 \end{matrix} \pmod{\chi_0 (= \chi^q)}.$$

This concludes our section on the groups of order PQ.

III. Applications of Representation Method.

In this section, we shall use the first method described in this paper to describe the unit groups of S_3, D_4 and D_6, and, as well, give a brief expository account of the findings for A_4.

A. The Unit Group of $\mathbb{Z}S_3$.

The first thing we do is consider a map deduced from a representation of S_3 given by

$$\theta(1\ 2) = \begin{pmatrix} 1, & -1, \begin{pmatrix} 1, & -1 \\ 0, & -1 \end{pmatrix} \end{pmatrix}$$

$$\theta(1\ 2\ 3) = \begin{pmatrix} 1, & 1, \begin{pmatrix} 0, & -1 \\ 1, & -1 \end{pmatrix} \end{pmatrix}$$

As one can see from the above this gives rise to a map

$$\theta: \mathbb{Q}S_3 \rightarrow \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}_2$$

We define the map by linear extension using the convention that cycles multiply from the right to the left (for example $(1\ 2)(1\ 2\ 3) = (2\ 3)$). Since we have defined θ by linear extension we see that this map is a homomorphism.

Let $B_1 = \{e, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ be a basis of $\mathbb{Q}S_3$ and let $\alpha = (\alpha_1, \alpha_2,...,\alpha_6)$ be an element of $\mathbb{Q}S_3$ with respect to the basis B_1. Similarly let B_2 be the canonical basis for $\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}_2$ with $X = (x_1,x_2,...,x_6)$ being an element of that space with respect to B_2.

Then we may consider $X = \theta\alpha = \alpha A$ where,

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 0 \end{bmatrix}$$

and upon further calculation we see that

$$A^{-1}=1/6\begin{bmatrix}1&1&1&1&1&1\\1&-1&-1&-1&1&1\\2&2&-2&0&-2&0\\0&0&-2&2&-2&2\\0&-2&0&2&2&-2\\2&-2&2&0&0&2\end{bmatrix}$$

As A is invertible, it is readily seen that θ is an isomorphism. Moreover from the elements of A it is readily seen that

$$\theta\mathbb{Z}S_3\subset\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}_2.$$

Furthermore, if we consider A^{-1}, then for $x_i\in\mathbb{Z}$, we have $\theta^{-1}x\in\mathbb{Z}S_3$ if and only if

$$\begin{aligned}
&x_1+x_2+2x_3 &&&&&&+2x_6\equiv 0(\text{mod } 6)\\
&x_1-x_2+2x_3 &&&&-2x_5&&-2x_6\equiv 0(\text{mod } 6)\\
&x_1-x_2-2x_3&&-2x_4&&&&+2x_6\equiv 0(\text{mod } 6)\\
&x_1-x_2 &&+2x_4&&+2x_5&&\equiv 0(\text{mod } 6)\\
&x_1+x_2-2x_3&&-2x_2&&+2x_5&&\equiv 0(\text{mod } 6)\\
&x_1+x_2 &&+2x_4&&-2x_5&&-2x_6\equiv 0(\text{mod } 6)
\end{aligned}$$

After simple row reduction we see that this reduces to the following set of three equations.

$$\begin{aligned}
&x_1+x_2 &&+2x_4&&+4x_5&&+4x_6\equiv 0(\text{mod } 6)\\
&4x_2 &&&&+4x_5&&+2x_6\equiv 0(\text{mod } 6)\\
&&4x_3&+2x_4&&+4x_5&&+2x_6\equiv 0(\text{mod } 6)
\end{aligned}$$

The second and third reduce respectively to:

$$x_2\equiv x_6-x_5(\text{mod } 3) \text{ and}$$

$$x_4+x_6\equiv x_3+x_5(\text{mod } 3)$$

Inspection of the first equation shows us that

$$x_1+x_2\equiv 0(\text{mod } 2)$$

If we also consider our first equation as an equation modulo 3 and combine it with the result of the second equation we get

$$x_1\equiv x_4+x_6(\text{mod } 3)$$

Therefore, the final result is as follows:

$$\begin{aligned}
&x_1+x_2\equiv 0(\text{mod } 2)\\
&x_2\equiv x_6-x_5(\text{mod } 3)\\
&x_1\equiv x_3+x_5\equiv x_4+x_6(\text{mod } 3)
\end{aligned}$$

Keeping all this in mind, we next consider the projection operator $\phi:\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}_2\to\mathbb{Q}_2$. Then we can see that

$$\phi\theta\mathbb{Z}S_3 = \left\{ \begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} \mid x_3+x_5 \equiv x_4+x_6 (\text{mod } 3) \right.$$

Let us call this space **Y**.

Let $X=(x_1,\ldots,x_6)\epsilon\theta\mathbb{Z}S_3$, with $x_6\equiv x_3+x_5 - x_4(\text{mod } 3)$. Let $\delta=x_3x_6 - x_4x_5$. Consider

$$(x_3 - x_4)(x_3+x_5) = x_3(x_3+x_5 - x_4) - x_4x_5 \equiv x_3x_6 - x_4x_5 \equiv \delta(\text{mod } 3)$$

In consideration of our row reduced equations it follows that X^{-1} exists and is in $\theta\mathbb{Z}S_3$ $<=>$ $x_3x_6 - x_4x_5=\delta=\pm 1$, $x_1=\pm 1$, $x_2 = \delta x_1$.

We see by composition of maps, that $\phi\theta$ is a homomorphism of $\mathbb{Z}S_3$ into **Y**, and therefore induces a homomorphisim of the unit group of $\mathbb{Z}S_3$ into the unit group of **Y**. We will now show that this induced homomorphism is one to one and onto, proving that it is an isomorphism.

Let

$$Z=\begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} \epsilon\, \mathcal{U}\mathbf{Y}.$$

Also let $\delta=x_3x_6 - x_4x_5=\pm 1$ and if $x_1,x_2 \epsilon \{-1,0,1\}$ are defined by the congruences

$$x_2\equiv x_6 - x_5 \text{ (mod 3) and}$$
$$x_1\equiv x_3+x_5 \text{ (mod 3)}$$

then neither x_1 nor x_2 is zero and all the above conditions are satisified. Therefore $\alpha=\theta^{-1}X$ is a unit in $\mathbb{Z}S_3$ with $\phi\theta\alpha=Z$. Therefore, by the above we have that $\phi\theta$ is one to one and onto therefore we have

Theorem 1.
The unit group of $\mathbb{Z}S_3$ is isomorphic to:

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \epsilon\, \mathcal{U}(\mathbb{Z}_2) \mid a+c \equiv b+d \text{ (mod 3)} \right\}$$

B. The units of $\mathbb{Z}D_4$

In this section, we will determine the group of units of $\mathbb{Z}D_4$, where D_4 is the dihedral group of order 8. This group is determined by the generators a,b together with the relations

$$a^4=b^2=baba=1.$$

Before proceeding with the construction, we give a few definitions. The homomorphism $\xi:\mathbb{Z}G\to\mathbb{Z}$ with $\xi(g)=1$ for all $g\in G$ is called the *augmentation function*. Denote by $V(\mathbb{Z}G)$ the normal subgroup of the units $u\in\mathbb{Z}G$ such that $\xi(u)=1$. If u is in $V(\mathbb{Z}G)$, it is called a *normalized unit*. Finally an automorphism θ of $\mathbb{Z}G$ is said to be normalized if $\xi\theta(g)=1$ for all g in G.

Now, as before, we determine our map from $\mathbb{Q}D_4$ to a direct sum of matrix rings over $\mathbb{Q}$. In this case, the map will be

$$\theta:\mathbb{Q}D_4\to\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}_2$$

given by

$$\theta(a)=\left(1,\ 1,\ -1,\ -1,\ \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right)$$

$$\theta(b)=\left(1,\ -1,\ 1,\ -1,\ \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\right)$$

In the same manner as before, consider D_4 as the basis of $\mathbb{Q}D_4$ and use the canonical basis for the right hand side of the above mapping. Then the map θ can be represented by A where A is the following matrix.

$$\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 & 1\\
1 & 1 & -1 & -1 & 0 & -1 & 1 & 0\\
1 & 1 & 1 & 1 & -1 & 0 & 0 & -1\\
1 & 1 & -1 & -1 & 0 & 1 & -1 & 0\\
1 & -1 & 1 & -1 & 0 & 1 & 1 & 0\\
1 & -1 & -1 & 1 & -1 & 0 & 0 & 1\\
1 & -1 & 1 & -1 & 0 & -1 & -1 & 0\\
1 & -1 & -1 & 1 & 1 & 0 & 0 & -1
\end{bmatrix}$$

Continuing our calculations we find that A^{-1} is $\frac{1}{8}$ times the following matrix.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 2 & 0 & -2 & 0 & 0 & -2 & 0 & 2 \\ 0 & -2 & 0 & 2 & 2 & 0 & -2 & 0 \\ 0 & 2 & 0 & -2 & 2 & 0 & -2 & 0 \\ 2 & 0 & -2 & 0 & 0 & 2 & 0 & -2 \end{bmatrix}.$$

In the same manner as before, we see that if

$$X=(x_1,x_2,x_3,x_4,\begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix})$$

with $X\epsilon\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}_2$, then X belongs to $\theta(\mathbb{Z}D_4)$ <=>

$$x_1+x_2+x_3+x_4+2x_5 \qquad +2x_8\equiv 0(\text{mod}8)$$

•

•

•

•

•

•

$$x_1 - x_2 - x_3+x_4+2x_5 \qquad - 2x_8\equiv 0(\text{mod } 8)$$

Applying row reduction in the same manner as the last example we get

i) $x_1+x_2+x_3+x_4+2x_5 \qquad +2x_8\equiv 0(\text{mod } 8)$

ii) $x_2+x_3 \qquad +2x_8\equiv 0(\text{mod } 4)$

iii) $x_3 - x_4 - x_5 - x_6 - x_7+x_8\equiv 0(\text{mod } 4)$

iv) $x_4+x_5 \quad +x_7 \quad \equiv 0(\text{mod } 2)$

v) $x_5 \quad +x_8\equiv 0(\text{mod } 2)$

vi) $x_6+x_7 \quad \equiv 0(\text{mod } 2)$

In addition, if X is to belong to $\theta(U(\mathbb{Z}D_4))$, then $x_i=\pm 1$, for i=1,2,3,4 and we must have $x_5x_8 - x_6x_7=\pm 1$.

Consider $\mathcal{X}\epsilon GL(2,\mathbb{Z})$, with

$$\mathcal{X}=\begin{pmatrix} x_5, & x_6 \\ x_7, & x_8 \end{pmatrix}$$

which satisfy equations v) and vi). Then there exists x_i, i=1,2,3,4 with

$$X=(x_1,x_2,x_3,x_4,\mathcal{X}) \in \theta(\mathcal{U}(\mathbb{Z}D_4) <=> \text{ one of a, b, or c hold.}$$

a) $x_8 \equiv 1 \pmod 2$; $x_5+x_6+x_7 - x_8 \equiv 0 \pmod 4$; $x_5+x_8 \equiv 2 \pmod 4$

b) $x_8 \equiv 1 \pmod 2$; $x_5+x_6+x_7 - x_8 \equiv 2 \pmod 4$; $x_5+x_8 \equiv 0 \pmod 4$

c) $x_8 \equiv 0 \pmod 2$; $x_5+x_8 \equiv 0 \pmod 4$

Let us do the calculations that show this. Consider; if X is in $\theta\mathcal{U}\mathbb{Z}D_4$, then, as noted before, we must have x_1,x_2,x_3 and $x_4 = \pm 1$. Let $\delta = \pm 1$. Then there are only certain combinations of the above that satisfy equations i) through vi). In particular, it should be noted that either all of x_1 to x_4 are either of the same sign or there are two of one sign and two of the other. To see this, consider equations i) and v). If three of x_1 to x_4 were +1 and the fourth -1, then we would have that $x_5+x_8 \equiv 1 \pmod 4$. This is an obvious contradiction to equation v).

Therefore, let us consider the cases separately. If $x_1=x_2=x_3=x_4=\delta$, then equation i) implies that

$$2x_5+2x_8 \equiv 4 \pmod 8 \text{ which implies that}$$
$$x_6+x_8 \equiv 0 \pmod 4.$$

Equation iii) tells us that

$$- x_5 - x_6 - x_7+x_8 \equiv 0 \pmod 4 \text{ which implies that}$$
$$x_5+x_6+x_7 - x_8 \equiv 0 \pmod 4.$$

Finally, equation ii) gives us that

$$x_8 \equiv 1 \pmod 2.$$

It can be readily seen that the above is condition a).

Let us now consider $x_1=x_2= - x_3 - x_4=\delta$. Here we see that equation i) implies

$$x_5+x_8 \equiv 0 \pmod 4.$$

Equation ii) implies

$$x_8 \equiv 0 \pmod 2.$$

We see that we now have condition c). In addition, however, we can see that equation iii) implies that

$$x_5+x_6+x_7 - x_8 \equiv 0 \pmod 4.$$

Now suppose that $x_1= - x_2=x_3= - x_4=\delta$. Then, we will have equation i) implying

$$x_5+x_8 \equiv 0 \pmod 4.$$

Equation ii) gives us

$$x_8 \equiv 0 \pmod 2.$$

Again, we have condition c). This time, though, Equation iii) shows us

$$x_5+x_6+x_6 - x_8 \equiv 2(\text{mod } 4).$$

Finally the last combination to consider is $x_1 = -x_2 = -x_3 = x_4 = \delta$. In this case we get equation i) showing that

$$x_5+x_8 \equiv 0(\text{mod } 4).$$

Equation ii) implies that

$$x_8 \equiv 1(\text{mod } 2).$$

Equation iii) implies that

$$x_5+x_6+x_7 - x_8 \equiv 2(\text{mod } 4).$$

This finally is condition b).

To show the other direction of the if and only if above is quite simple given the above calculations. What one needs to do is to simply choose the particular x_i $(i=1,2,3,4)$ as is given above. These will then satisfy all the equations.

Let us denote by Ω those matrices of $GL(2,\mathbb{Z})$ that satisfy equations v) and vi) above and any one of a), b) or c). It is obvious by the linearity of the constraints that Ω is a subgroup of $GL(2,\mathbb{Z})$. For any element $X \epsilon \Omega$ we can see by the above computations that there are exactly two elements of $\theta\mathcal{U}(\mathbb{Z}D_4)$ with X as the last member.

Let $\delta = \pm 1$ as above.

If a) holds, then $X=(\delta,\delta,\delta,\delta,\mathcal{X}) \epsilon \theta\ (\mathcal{U}(\mathbb{Z}D_4))$.

If b) holds, then $X=(\delta,-\delta,-\delta,\delta,\mathcal{X}) \epsilon \theta\ (\mathcal{U}(\mathbb{Z}D_4))$.

If c) holds, there are two cases to consider. If we have the first, which is

$$x_5+x_6+x_7 - x_8 \equiv 0(\text{mod } 4)$$

holding, then

$$X=(\delta,\delta,-\delta,-\delta,\mathcal{X}) \epsilon \theta\ (\mathcal{U}(\mathbb{Z}D_4)).$$

Otherwise, we have

$$x_5+x_6+x_7 - x_8 \equiv 2(\text{mod } 4)$$

holding which gives us

$$X=(\delta,-\delta,\delta,-\delta,\mathcal{X}) \epsilon \theta\ (\mathcal{U}(\mathbb{Z}D_4)).$$

Now, we are in a position to describe the unit group of $\mathbb{Z}D_4$. If we choose $\alpha \epsilon \mathcal{U}(\mathbb{Z}D_4)$ such that $\theta(\alpha)=(x_1,x_2,x_3,x_4,\mathcal{X})$, then we can observe that $\xi(\alpha)=x_1$. From this and the preceding information it is easy to see that since for any element $\mathcal{X}$ in Ω there are exactly two elements in $\theta\mathcal{U}(\mathbb{Z}D_4)$ we have the theorem.

Theorem.

$$\mathcal{U}(\mathbb{Z}D_4) \cong \{\pm 1\} \times \Omega.$$

C. Units of $\mathbb{Z}D_6$

In this section, we will show how a minor extension to the method of this section can be used to describe unit groups of group rings over $\mathbb{Z}$, where the groups are of higher orders. At this point, we will determine the unit group of $\mathbb{Z}D_6$ where D_6 is the dihedral group of order 12 given by the generators a,b together with the relations

$$\{ a^2 = b^6 = ab^2ab^2 = e \}$$

Now if we applied the method of this section blindly we would be dealing with matrices of order 12. This, to say the least, is inelegant. In addition to this the description of $\mathcal{U}(\mathbb{Z}D_6)$ would include a direct product of two matrix groups. This does not give us a very satisfying description, as determining properties of this type of product is not very easy.

Instead, what we do in this section is to consider $D_6 \cong C_2 \times S_3$, where C_2 is the cyclic group of order 2, $=\{+1, -1\}$ under multiplication. S_3 is, as before, the symmetric group on 3 elements. Keeping this in mind, we have $\mathbb{Z}D_6 \cong (\mathbb{Z}C_2)S_3$, where $\mathbb{Z}C_2$ is the group ring of the group C_2 over the ring $\mathbb{Z}$, and the whole thing is the group ring of the group S_3 over the ring $\mathbb{Z}C_2$.

At this point, let us denote $\mathbb{Q}C_2$ by $\mathcal{R}$. Then what we intend to do is to apply the method used previously, replacing $\mathbb{Q}$ by $\mathcal{R}$ and $\mathbb{Z}$ by $\mathbb{Z}C_2$.This brings us to the point where we may now define the map

$$\theta: \mathcal{R}S_3 \to \mathcal{R} \oplus \mathcal{R} \oplus \mathcal{R}_2$$

by

$$\theta(1\ 2) = \left(1, -1, \begin{pmatrix} 1, & -1 \\ 0, & -1 \end{pmatrix}\right)$$

and

$$\theta(1\ 2\ 3) = \left(1, 1, \begin{pmatrix} 0, & -1 \\ 1, & -1 \end{pmatrix}\right)$$

At this point, one must keep in mind that the elements of the above vectors are in $\mathcal{R}$ not in $\mathbb{Q}$ as before.

Now, let us consider the two modules $\mathcal{R}S_3$ and $\mathcal{R} \oplus \mathcal{R} \oplus \mathcal{R}_2$. The first $\mathcal{R}S_3$ is obviously a free module over $\mathcal{R}$ with basis the elements of S_3. The second is again a free module over $\mathcal{R}$

being a direct sum of matrix rings over $\mathcal{R}$. We will use the standard basis for this module.

Considering this, we may look at θ as a module homomorphism between two free modules. We may therefore represent it as a matrix A, in this case, a 6 by 6 matrix. Obviously this matrix is going to have the same entries as the one we obtained when looking at $\mathbb{Z}S_3$, with the distinction that these elements will be in $\mathcal{R}$ and not just in $\mathbb{Q}$. For the sake of convenience I will rewrite A and A^{-1}.

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & -1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 0 & -1 & 1 \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 0 \end{bmatrix}$$

and

$$A^{-1} = 1/6 \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & 1 \\ 2 & 2 & -2 & 0 & -2 & 0 \\ 0 & 0 & -2 & 2 & -2 & 2 \\ 0 & -2 & 0 & 2 & 2 & -2 \\ 2 & -2 & 2 & 0 & 0 & 2 \end{bmatrix}$$

As before, since A is invertible we see that θ is an isomorphism. Also, as before, we are led to a set of six congruences that describe when an element of $(\mathbb{Z}C_2)\oplus(\mathbb{Z}C_2)\oplus(\mathbb{Z}C_2)_2$ mapped by θ^{-1} is in $(\mathbb{Z}C_2)S_3$. It is not neccessary to re-write the original equations. The result after row reduction are the equations:

$$x_1 + x_2 \equiv 0 (\text{mod } 2)$$
$$x_2 \equiv x_6 - x_5 (\text{mod } 3)$$
$$x_1 \equiv x_3 + x_5 \equiv x_4 + x_6 (\text{mod } 3)$$

At the risk of being repetitious, we note that the above congruences are in $\mathbb{Z}C_2$. Namely that we are considering modulo the ideals generated by 2 or 3 in $\mathbb{Z}C_2$ in the above equations.

Let ϕ denote the projection map of $\mathcal{R}\oplus\mathcal{R}\oplus\mathcal{R}_2$ onto $\mathcal{R}_2$. Then we have that

$$\phi\,\theta((\mathbb{Z}C_2)S_3) = \left\{\begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix}: x_3+x_5 \equiv x_5+x_6 \pmod 3\right\}$$

Let us call the above set $\mathcal{Y}$.

Let us now pause for a moment to consider some of the properties of $\mathbb{Z}C_2$, where e is the identity of C_2 and η is the other element with $\eta^2=e$. The units of the group ring $\mathbb{Z}C_2$ are easy to determine as they are only $\pm C_2$. Therefore, for a matrix to be in the units of $(\mathbb{Z}C_2)_2$ the determinant must be one of $\pm e$ or $\pm\eta$.

If $X=(x_1,\ldots,x_6)$ is in $\theta(\mathbb{Z}C_2)S_3$, then, if we let δ represent any one of $\pm e$, $\pm\eta$, then as was calculated before, we have that X^{-1} exists and is in $\theta(\mathbb{Z}C_2)S_3$ if and only if

$$x_3x_6-x_4x_5=\delta,\ x_1=\delta,\ x_2=\pm\delta.$$

The mapping $\phi\theta$ is a ring homomorphism of $(\mathbb{Z}C_2)S_3$ into $\mathcal{Y}$ and thus induces a homorphism from $\mathcal{U}((\mathbb{Z}C_2)S_3 \to \mathcal{U}(\mathcal{Y})$. I claim that this is an isomorphism. To see this let

$$\mu = \begin{pmatrix} x_3 & x_4 \\ x_5 & x_6 \end{pmatrix} \in \mathcal{Y}.$$

Then $\delta=x_3x_6-x_4x_5=\pm e$ or $=\pm\eta$ and if we choose x_1,x_2 which are in $\{e, 0, -e, \eta, -\eta\}$ to satisfy

$$x_2 \equiv x_6 - x_5 \pmod 3$$
$$x_1 \equiv x_3+x_5 \pmod 3,$$

it follows from this that neither x_1 nor x_2 is 0 and that the above conditions are all satisfied. Thus $\alpha=\theta^{-1}X$ is a unit in $(\mathbb{Z}C_2)S_3$ with $\phi\theta\alpha=\mu$. Furthermore, we can see that from the preceding conditions that $\phi\theta$ is one-to-one.

Therefore, remembering that $\mathbb{Z}D_6 \cong (\mathbb{Z}C_2)S_3$ and that $\mathcal{U}(\mathbb{Z}D_6) \cong \mathcal{U}((\mathbb{Z}C_2)S_3)$ we have the following theorem.

THEOREM.

$$\mathcal{U}(\mathbb{Z}D_4) \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{U}((\mathbb{Z}C_2)_2): a+c \equiv b+d \pmod 3 \right\}.$$

D. The Unit Group of $\mathbb{Z}A_4$,(expository)

In this section, we will present the characterization of $\mathcal{U}(\mathbb{Z}A_4)$ as presented by Allen and Hobby[1]. We will not include the proofs, as it is felt that nothing new is to be gained from presenting the method a fourth time.

As is known A_4 has 4 irreducible representations, call them θ_i $i=1,2,3,4$. Also A_4 is generated by the two elements $a=(1\ 2)(3\ 4)$ and $b=(1\ 2\ 3)$. The representations θ_i $i=1,2,3$ are

easily described as follows. $\theta_i(a)=1$ and $\theta_i(b)=\omega^{i-1}$. The fourth, θ_4, is given as follows

$$\theta_4(a)=\begin{bmatrix}-1&0&1\\-1&0&1\\-1&1&0\end{bmatrix} \quad \text{and } \theta_4(b)=\begin{bmatrix}-1&1&0\\-1&0&0\\-1&0&1\end{bmatrix}$$

Let $\theta:\mathbb{Q}A_4\rightarrow\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}\oplus\mathbb{Q}_3$ be defined by $\theta(r)=(\theta_1(r),\theta_2(r),\theta_3(r),\theta_4(r))$. Then we may use this map as in the preceding sections to determine the unit group. The characterization arrived at by Allen and Hobby is as follows.

THEOREM

$\mathcal{U}(\mathbb{Z}A_4)\cong\{\pm1\}\times\{X\in SL(3,\mathbb{Z})$: such that X satisfy the below conditions 1, 2, and 3.$\}$

1. Every column sum of X is congruent to 1(mod 4).
2. No row contains all odd elements, and
3. One pseudo-trace is congruent to -1(mod 4) while the other two are congruent to 0(mod 4).

There are three pseudo-traces on a three by three matrix; they are the sums of the elements on the pseudo-diagonals that have been discussed previously.

IV. Groups of order 27

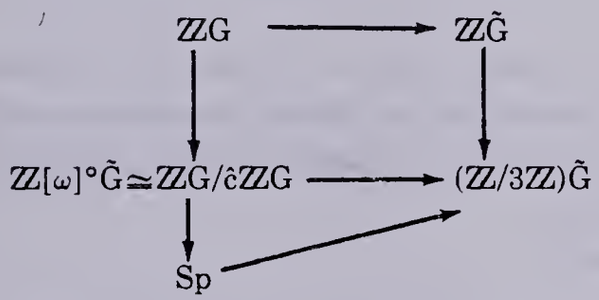
In this section, we will use the method presented earlier in the paper to determine the unit group of the integral group rings of the two non-commutative groups of order 27.
Recall,

$$G = \langle a,b \mid (a,b) = c,\ ca = ac,\ cb = bc,\ a^3 = b^3 = c^3 = 1\rangle, \text{ and}$$
$$H = \langle a,b \mid a^9 = b^3 = 1,\ b^{-1}ab = a^4\rangle.$$

As is true in general, we have that $\tilde{G} = \langle\tilde{a}\rangle\times\langle\tilde{b}\rangle$, and $\tilde{H} = \langle\tilde{a}\rangle\times\langle\tilde{b}\rangle$ are both elementary abelian 3-groups. Recall, from our previous work that $\mathcal{U}\mathbb{Z}\tilde{G} = \pm\tilde{G}$ and $\mathcal{U}\mathbb{Z}\tilde{H} = \pm\tilde{H}$. The object of this section is to give a concrete description of both $\mathcal{U}\mathbb{Z}G$ and $\mathcal{U}\mathbb{Z}H$.

A. First group of order 27.

Let us consider G first. Referring back to our general proof we would let $A = \mathrm{DIAG}(1,\omega,\omega^2)$ and $B = \mathrm{PDIAG}_1$. Our fibre product diagram would become



In the above the map from Sp to $(\mathbb{Z}/3\mathbb{Z})\tilde{G}$ is denoted by ϕ_1 and the map from $\mathbb{Z}G/\hat{c}\mathbb{Z}G$ to Sp is denoted by ϕ_0. These maps are defined in the same way as they were in general. Specializing the condition (*) from the general theorem we see that the matrix

$$M = \begin{bmatrix} x_{0,0} & x_{1,0} & x_{2,0} \\ x_{2,1} & x_{0,1} & x_{1,1} \\ x_{1,2} & x_{2,2} & x_{0,2} \end{bmatrix} \in \mathbb{Z}[\omega]_3$$

belongs to our Sp if and only if for each i, $0\leq i\leq 2$, the conditions

$$x_{i,0} + x_{i,1} + x_{i,2} \in 3\mathbb{Z}[\omega]$$
$$x_{i,0} + x_{i,1}\omega + x_{i,0}\omega^2 \in 3\mathbb{Z}[\omega]$$
$$x_{i,0} + x_{i,1}\omega^2 + x_{i,2}\omega \in 3\mathbb{Z}[\omega]$$

hold. To find $\phi_1(M)$, we need $a_{i,j}\in\mathbb{Z}[\omega]$ such that $M = \sum a_{i,j}A^iB^j$. This will give us the matrix equations

$$\begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \end{bmatrix} = \tfrac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix} \begin{bmatrix} x_{j,0} \\ x_{j,1} \\ x_{j,2} \end{bmatrix}$$

and this is equivalent to

$$(**) \qquad \begin{aligned} a_{0,j} &= \tfrac{1}{3}(x_{j,0}+x_{j,1}+x_{j,2}) \\ a_{1,j} &= \tfrac{1}{3}(x_{j,0}+\omega^2 x_{j,1}+\omega x_{j,2}) \\ a_{2,j} &= \tfrac{1}{3}(x_{j,0}+\omega x_{j,1}+\omega^2 x_{j,2}) \end{aligned}$$

From our previous work we know that $\phi_1(M) = \sum \tilde{a}_{i,j}\tilde{a}^i\tilde{b}^j$. Also, we know that the units of $\mathbb{Z}G$ are pairs (α, M), with $\alpha \epsilon \mathcal{U}\mathbb{Z}\tilde{G}$ and M in Sp with $\phi_1(M) = \phi_2(\alpha)$. However, since we know that $\mathcal{U}\mathbb{Z}\tilde{G} = \pm\tilde{G}$, we need matrices M such that

$$\phi_1(M) = \sum \tilde{a}_{i,j}\tilde{a}^i\tilde{b}^j = \theta_2(\pm a^m b^n)$$

for some m,n. If we put $\chi = \omega - 1$ then we get

1. For two values of i and all j, $a_{i,j} \equiv 0 \pmod{\chi}$.
2. Considering the third value for i, either $a_{i,0} = \pm 1$, $a_{i,1} \equiv a_{i,2} \equiv 0 \pmod{\chi}$ or
   $a_{i,1} = \pm 1$, $a_{i,0} \equiv a_{i,2} \equiv 0 \pmod{\chi}$ or
   $a_{i,2} = \pm 1$, $a_{i,0} \equiv a_{i,1} \equiv 0 \pmod{\chi}$.

This proves the following theorem.

THEOREM.
$\mathcal{U}\mathbb{Z}G \cong \{M \epsilon \mathcal{U}\mathbb{Z}[\omega]_3 \mid M$ satisfies 1. and 2. where $a_{i,j}$ are given by $(**)\}$.

From the above it is clear that the matrices in $\mathcal{U}\mathbb{Z}[\omega]_3$ which are congruent to I (mod χ^3) are contained in $\mathcal{U}\mathbb{Z}G$ and therefore, $\mathcal{U}\mathbb{Z}G$ is a congruence subgroup in $SL(3,\mathbb{Z}[\omega])$.

Second group of order 27

Now, let us describe $\mathcal{U}\mathbb{Z}H$. If we have a matrix

$$X = Z' = \begin{bmatrix} x_{0,0} & x_{1,0} & x_{2,0} \\ x_{2,1} & x_{0,1} & x_{1,1} \\ x_{1,2} & x_{2,2} & x_{0,2} \end{bmatrix}$$

satisfying (*) then the corresponding matrix in Sp is

$$Z = \begin{bmatrix} x_{0,0} & x_{1,0} & x_{2,0} \\ \omega x_{2,1} & x_{0,1} & x_{1,1} \\ \omega x_{1,2} & \omega x_{2,2} & x_{0,2} \end{bmatrix}$$

If we write $A = \Sigma a_{i,j} B^i A^j$, then $\phi_1(Z) = \pm h$, $h \in H$ if and only if the matrix X satisfies 1. and 2. from above. Then we have the the following theorem.

THEOREM.
$\mathcal{U}\mathbb{Z}H \cong \{Z \in \mathcal{U}\mathbb{Z}[\omega]_3 | Z' \text{ satisfies 1. and 2. where } a_{i,j} \text{ are given by (**)}\}$.

Again it is easily seen that $\mathcal{U}\mathbb{Z}H$ is a congruence subgroup in $SL(3,\mathbb{Z}[\omega])$.

References

[1] P. J. Allen and C. Hobby, A characterization of units in $\mathbb{Z}[A_4]$, J. Algebra 66 (1980), 534-543.

[2] I. Hughes and K. R. Pearson, The group of units of the integral group ring $\mathbb{Z}S_3$, Canad. Math. Bull. 15 (1972), 529-534.

[3] I. S. Luthar, Units in integral group rings, To appear.

[4] C. Polcino-Milies, The units of the integral group ring $\mathbb{Z}D_4$, Bol. Soc. Brasil. Mat. 4(1972),85-92.

[5] J. Ritter and S. K. Sehgal, Integral group rings of some p-groups, To appear.

[6] S. K. Sehgal, Topics in Group Rings, Dekker, New York, 1978. (Chapter 2) [7] Ullom, Reiner, and Gallovich, Class Group for Integral Representations of Meta-cyclic Groups, Mathematika 19, 1972, 105-111.